Improving the Physical and Environmental Security of a Data Centre: Case Study of a Hong Kong Wines and Spirits Distribution Company

Hon Keung Yau, Alison Lai Fong Cheng

***Abstract* — The purpose of this paper is to provide solutions to improve the physical and environmental security of a data centre for a Hong Kong wines and spirits distribution company. Documentation method was employed. Finally the physical environment of the data centre was improved and one set of physical and environment policy was established.**

***Index Terms* — Data centre, Hong Kong, Physical and environmental security.**

I. INTRODUCTION

This paper studies the physical and environmental security of a data centre of a Hong Kong wines and spirits distribution company. This company is responsible for the distribution of wines and spirits to most South Asia's countries, including China, Hong Kong, Singapore, Malaysia, Thailand, Vietnam, Laos, Cambodia, Indonesia and Philippines. This company has a small data centre in Hong Kong. However, the physical and environmental condition of this data centre was not very good and no physical and environmental security policy was developed for this centre. We were invited to act as a consultant to design a plan to improve the physical and environmental security of this data centre.

II. LITERATURE REVIEW

This data security policy bases on ISO/IEC 27001:2005 standards and includes a lot of details and guidelines to solve or handle many security related problems. The policy comprehends nine parts including physical and environmental security. As described by IT Governance [2], ISO/IEC 27001:2005 is the best practice specification that helps businesses and organizations throughout the world to develop a best-in-class Information Security Management Systems (ISMS). Further to Calder [1], this evolution in the standard (ISO/IEC 27001:2005) now enables organizations throughout the world to ensure that they are applying information security best practice in their organizations. The ISO 27001:2005 ISMS standard considers everything about risk which specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. The three core principles involved are confidentiality, integrity and availability. These principles cover physical and environmental security.

Manuscript received August 18, 2013

H. K. Yau is with the Department of Systems Engineering and Engineering Management, City University of Hong Kong, Kowloon Tong, Kowloon, Hong Kong (corresponding author to provide phone: 852-34426158, Fax: 852-34420173, email: honkyau@cityu.edu.hk).

A. L. F. Cheng is an independent researcher (email: alisoncheng_lai_fong@yahoo.com.hk).

III. METHODOLOGY

According to Legal Advantage [3], documentation is a very important part of discovery process in litigation, contracts, mergers and acquisitions. Thus, document review and analysis will be used most of the time in this project. It is to collect information from existing documentations of the company, reference books and online reference. Many of these documents give ideas about existing technology, methods of management used or future development or trends of technology or skills.

IV. RESULTS AND DISCUSSION

This section consists of two parts: (1) A better physical environment data centre was set up; (2) A physical and environmental policy was established.

A better physical environment data centre was set up.

A. Physical layout

A data center can occupy one room, one or more floors, or even an entire building. Most of the equipment is often in the form of servers mounted in 19 inch rack cabinets (Figure 1), which are placed in single rows forming corridors between them. In this way, people can access the front and rear of each cabinet. Servers differ greatly in size from 1U servers to large freestanding storage silos which occupy many tiles on the floor. Some equipment such as mainframe computers and storage devices are often as big as the racks themselves, and are placed alongside them. Very large data centers may use shipping containers packed with 1,000 or more servers each; when repairing or upgrading, whole containers are replaced (rather than repairing individual servers). Most of the times, local building codes govern the minimum ceiling heights. The physical environment of a data center is rigorously controlled:

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Figure 1- A typical server rack

B. Air Conditioning & Humidity

Air conditioning is used to control the temperature and humidity in the data center. ASHRAE's "Thermal Guidelines for Data Processing Environments" recommends a temperature range of 16–24 °C (61–75 °F) and humidity range of 40–55% with a maximum dew point of 15°C as optimal for data center conditions. The electrical power used heats the air in the data center. Electronic equipment malfunction will be resulted as the ambient temperature will rise unless the heat is removed. By controlling the air temperature, the server components at the board level are kept within the manufacturer's specified temperature/humidity range. Air conditioning systems help control humidity by cooling the return space air below the dew point.

Too much humidity and water may begin to condense on internal components. In case of a dry atmosphere, ancillary humidification systems may add water vapor if the humidity is too low, static electricity discharge problems may be resulted and damage components. Subterranean data centers may keep computer equipment cool while expending less energy than conventional designs.

Modern data centers try to use economizer cooling, where they use outside air to keep the data center cool. A few data centers in Washington cool all of the servers using outside air 11 months out of the year.. Without using chillers/air conditioners, they create potential energy savings in the million dollars.

C. Power Supply

Power Supply plays a large role with data centre, so backup power supply is essential. Backup power consists of one or more uninterruptible power supplies and/or diesel generators (Figure 2).

To prevent single points of failure, all elements of the electrical systems, including backup system, are typically fully duplicated, and critical servers are connected to both the "A-side" and "B-side" power feeds. This arrangement is often made to achieve N+1 Redundancy in the systems. Static switches are sometimes used to ensure instantaneous switchover from one supply to another in the event of a power failure or blackout.

Figure 2 – A bank of batteries in a large data center, used to provide power until diesel generators can start

D. Fire Protection

Data centers feature fire protection systems, including passive and active design elements, as well as implementation of fire prevention programs in operations. Early warning of a developing fire are usually provided by installing smoke detectors which detect particles generated by smoldering components prior to the development of flame. This allows investigation, interruption of power, and manual fire suppression by hand held fire extinguishers before the fire grows to a large size. A fire sprinkler system is often used to control a full scale fire if it develops. Fire sprinklers require 18 in (46 cm) of clearance like free of cable trays below the sprinklers. Clean agent fire suppression gaseous systems can also be used to suppress a fire earlier than the fire sprinkler system. Passive fire protection elements include the installation of fire walls around the data center, so a fire can be restricted to a portion of the facility for a limited time in case of the failure of the active fire protection systems, or if they are not yet installed. These firewalls are often insufficient to protect heat-sensitive electronic equipment for critical facilities, however, because conventional firewall construction is only rated for flame penetration time, not heat penetration. Cable penetrations, coolant line penetrations and air ducts are also deficiencies in the protection of vulnerable entry points into the server room. For mission critical data centers fireproof vaults with a Class 125 rating are necessary to meet NFPA 75 standards.

E. Raised Flooring

Data centers typically have raised flooring made up of 60 cm (2 ft) removable square tiles. The trend is towards 80–100 cm (31–39 in) void to cater for better and uniform air distribution. As part of the air conditioning system, these provide a plenum for air to circulate below the floor, as well as providing space for power cabling. In modern data centers data cabling is typically routed through overhead cable trays. But still some recommend under raised floor cabling for security reasons and to consider the addition of cooling systems above the racks in case this enhancement is necessary. Smaller or less expensive data centers without

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

raised flooring may use anti-static tiles for a flooring surface. Computer cabinets are often organized into a hot aisle arrangement to maximize airflow efficiency.

F. Physical Security

Physical security is also a very important aspect in data centers. Physical access to the site is usually restricted to selected personnel, with controls including bollards and mantraps. If the data center is large or contains sensitive information on any of the systems within video camera surveillance and permanent security guards are almost always present. It's getting common to use finger print recognition man traps.

Figure 3. - Multiple racks of servers, and how a data center commonly looks.

G. Applications

A data center may be concerned with just operations architecture or it may provide other services as well.

The main purpose of a data center is running the applications that handle the core business and operational data of the organization. Such systems may be proprietary and developed internally by the organization, or bought from enterprise software vendors. Such common applications are ERP and CRM systems.

Often these applications will be composed of multiple hosts, each running a single component. Common components are databases, file servers, application servers, middleware, and various others (Figure 3).

Data centers are also used for off site backups. Companies may subscribe to backup services provided by a data center. This is often used in conjunction with backup tapes. Backups can be taken of servers locally on to tapes. However tapes stored on site can be a security threat and are also susceptible to fire and flooding. Larger companies may also send their backups off site for added security by backing up to a data center. Encrypted backups can be sent over the Internet to another data center where they can be stored securely.

For disaster recovery, several large hardware vendors such as Cisco Systems, Sun Microsystems, IBM and HP have developed mobile solutions that can be installed and made operational in very short period of time.

Data security has become increasingly important to all kinds of companies in this information era and thus a good data security policy is essential to ensure competitiveness of the company.

H. Physical and environmental Policy

This section covers the physical protection of buildings; access controls; environmental threats and controls to be applied in secure areas such as server rooms. The following sections are included (1) Physical Security Perimeter and Entry Control; (2) Protecting Against External and Environmental Threats; (3) Working in Secure Areas; and (4) Public Access, Delivery and Loading Areas

I. Physical Security Perimeter and Entry Control

The objective of this section is to use suitable and appropriate security perimeters or measures to protect company's office from unauthorized access. It also ensures information assets are protected from physical threats. The presence of unauthorized people in our back-office increases the risk of unauthorized access to our data either by unauthorized system access or by viewing information on screens or on paper.

The following procedures were considered and implemented::

1) Account must be taken of relevant health and safety regulations
2) Perimeters should be clearly defined that each measure used should be appropriate and proportion to the security level of the assets protected and the results of a risk assessment
3) Perimeters of any building housing information and systems should be physically sound with no gaps in the perimeter
4) External walls must be of solid construction
5) Doors with control mechanisms such as bars, alarms and locks should be used against unauthorized access
6) Windows should be locked and windows at ground level should have additional protection like intruder detection systems
7) Emergency exit doors should be fitted with an alarm, monitored and tested
8) The fire doors must operate in accordance with fire regulations
9) Systems managed by different parties should be physically separated
10) Additional barriers like staff card control access system should be implemented to control physical access between areas with different security levels
11) All staff must be identifiable by their staff card
12) All visitors must be issued visitor pass before entering the office
13) All visitors should be escorted by a member of company at anytime in the office
14) Special secure areas which require staff PIN or staff card like server rooms should not be accessible by unauthorized personnel or visitors.
15) Access rights to secure areas must be reviewed and updated regularly
16) Third party support personnel should be granted restricted access to secure areas only when necessary

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

J. Protecting Against External and Environmental Threats

The objective of this section is to design and apply physical protection against external and environmental threats. It also ensures that any possible damage from man-made or natural disasters is minimized.

Consideration should be given to the following to avoid damage from fire, flood, power outage, explosion, civil unrest, and other forms of natural or man-made disaster:

1) Hazardous or combustible materials should be stored appropriately and at a safe distance from any areas housing critical information or systems
2) Recovery equipment and back-up media should be sited at a distance away from the main site
3) Data centres should be used for fast recovery after damaging incidents
4) Fire fighting equipments should be installed and placed appropriately according to the law
5) Server rooms must NOT be used as storage areas especially paper or cardboard
6) All server and equipment racks must be affixed to an adjacent solid surface
7) All server rooms should have a positive pressure environment such that no extraneous material is blown into the server room
8) Floor tiling must be laid correctly and replaced immediately after any under floor work is completed

K. Secure Areas

The objective of this section is to identify and apply appropriate measures for the physical protection of secure areas. Secure areas such as locations such as server rooms, security rooms housing security equipment usually house business critical or sensitive systems, which need to be protected from accidental or malicious damage.

The following procedures were used to protect such areas:

1) Secure areas locations should be known on a need to know basis;
2) Unsupervised working in such areas should be avoided
3) Secure areas should be suitably locked and periodically checked
4) Only authorized personnel will be allowed access to secure areas.
5) Access to server rooms must be limited to the IT manager or their appointee and certain contractual IT staff.

L. Public Access, Delivery and Loading Areas

The objective of this section is to control access points such as reception, delivery and loading areas. It also ensures that people do not have direct access to office from publicly accessible place.

The following procedures were used:

1) Access to delivery and loading area from outside the building should be restricted to authorized and identified personnel by staff PIN or staff card
2) Incoming and outgoing materials should be recorded at point of entry and exit respectively and inspected for potential threats before it moves to point of use;
3) Incoming and outgoing shipments should be segregated where possible;
4) Reception must only allow entry to the office to authorized personnel or registered visitors

Based on documentation of different papers and study of the ISO standard, this Data Policy is created. This Policy can handle and deal with security problems of different aspects including physical security breaches, environmental damages recovery, access control management and electronic commerce safety problems.

This policy also gives clear guidelines to each aspect, step by step to solve the problem. These includes prevention of happening, monitoring usual practices, tackling security issues, implementation of planning, tracking of source of problem and recovery measures.

In order to achieve the expected effect of the policy, the co-operation of full implementation by staff and commitment by management teams is essential. Regular review should also be carried out to review the policy and keep it updated.

V. CONCLUSION

The physical environment of the data centre was improved and the physical and environmental policy was established in this study.

According to Calder [1], a good manager with excellent management skills is needed to implement this policy while the commitment of managers and staff and cooperation between them is another key to success.

A few parts were deleted from the original standard due to repetition and time limitation. The policy should later be extended to the parts not covered in this project. More analysis and testing should also be done to review, grade and comment on the actual performance and implementation rate of the policy. Management team should also study more about the standard to have clearer ideas and implementation of the standard and policy.

There were two limitations: Firstly, it is hard for company to reveal its current policies especially regarding security issues that less information can be gathered for this project. Secondly, most cases found from books or Internet are old cases and designed for foreign countries with very different Laws and regulations from Hong Kong that sometimes it is hard to apply the cases to a company operating in Hong Kong. Lastly, the actual effect and implementation are hard to measure and those statistics are usually highly confidential.

REFERENCES

[1] A. Calder, *Nine Steps to Success: An ISO 27001 Implementation Overview.* London: IT Governance Publishing, 2005

[2] IT Governance, The One-Stop-Shop for everything to do with IT Governance, http://www.itgovernance.co.uk/, 2010.

[3] Legal Advantage, The Document Review Process, http://legaladvantage.net/DocumentReviewProcess.aspx 2010

ISBN: 978-988-19253-3-6
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)